

REMARKS

Claims 1 - 12 remain in the application, and are amended herein.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

Section 101 Rejections

Claims 1 - 12 stand rejected under 35 U.S.C. §101 on the grounds that the claimed invention is only a manipulation of basic mathematical constructs. It is well established that "an application of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection." *Diamond v. Diehr*, 450 U.S. at 187, 209 USPQ at 8 (emphasis in original); accord *Parker v. Flook*, 437 U.S. at 590, 198 USPQ at 197; *Gottschalk v. Benson*, 409 U.S. at 67, 175 USPQ at 675. Thus, "[w]hile a scientific truth, or the mathematical expression of it, is not a patentable invention, a novel and useful structure created with the aid of knowledge of scientific truth may be." *Diehr*, 450 U.S. at 188, 209 USPQ at 8-9.

The MPEP establishes, at Chapter 2106, Section IV, subsection C, subsection (2), that a claimed invention is directed to a practical application, and therefore satisfies the requirements of 35 U.S.C. §101, when it "produces a useful, concrete and tangible result....."

As set forth in the Specification and Abstract, numerous processes and structures rely on the availability of random numbers to properly function. These processes and structures include simulation studies, information processing, communication systems, and structures for encryption of data. In each case, the effectiveness of the process or structure depends on having a source of random numbers for which it is effectively impossible to predict or anticipate the next appearing number when presented with only the existing set of random numbers. Use of typical methods of creating pseudo-random numbers to provide input sequences for such applications may undermine

the effectiveness of the application if the numbers being generated are repetitive or otherwise predictable. For example, using repeating sequences of numbers as input data for encryption provides a basis for predicting later input data, and thus a basis for breaking the code. The instant process and apparatus for generating random numbers does not create repetitive sequences of numbers. Therefore, numbers generated by the instant invention are highly **useful** in all applications requiring random numbers or pseudo-random numbers.

Similarly, the random numbers generated by the instant invention are **tangible**, since the numbers themselves have a practical application and are not merely abstract. As indicated in the Specification at page 6, the numbers generated by the claimed invention a.) may be successfully replicated at distinct locations and at different times, b.) are unpredictable in a manner comparable to purely random sequences, and c.) may be created in an unlimited supply. As a result, the sequences of numbers created by the claimed apparatus and method have numerous practical applications in the areas of simulation studies, information processing, communication, and encryption, as they provide a tangible and practical method of providing input for such applications and structures. Each process claim has been modified by this Reply to emphasize the practical application of the generated random numbers. The claims therefore more clearly establish the practical and tangible result of the claimed process.

Finally, the claimed invention is clearly repeatable, so that the result of employing the invention substantially produces the same result regardless of location or time (see Specification Page 6, lines 5-7). Therefore, the claimed process and apparatus meets the requirement of being **concrete**. (See MPEP Chapter 2106, Section IV, subsection C, subsection (2), subsection c)).

In light of the useful, tangible, and concrete results produced by the claimed invention, it is submitted that the claimed invention is directed to a practical application of a 35 U.S.C. §101 judicial exception.

Section 103 Rejections

Claims 1 - 12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over *Handbook of Applied Cryptography* by Menezes.

Sections 5.2 and 5.3 of Menezes teach the application of a one-way mathematical function sequentially to a set of values. This teaching does not include the application of a function simultaneously to both an initial number and a subsequent number. Therefore, while Menezes creates pseudo-random bit sequences, the claimed invention creates what have been defined in the Specification as idem-random numbers: numbers with the fundamental characteristics of random numbers, so that anticipation or prediction of the next sequential idem-random value is effectively impossible, given only the existing sequence of numbers. (See Specification page 3, lines 6-18).

Unlike the pseudo-random numbers created by the Menezes process, the idem-random numbers of the instant invention are not repeated in a cycle by the claimed process. As a result, the idem-random numbers of the instant invention may be utilized in applications which employ random numbers, effectively providing the unpredictability associated with truly random numbers.

Furthermore, Menezes does not teach the use of prime numbers as a source of input for his process, in contrast to the claimed invention.

The examiner cites Section 4.4.1 of Menezes for teaching a method for finding prime numbers that potentially includes establishing an initial prime number, establishing a subsequent prime number identification condition, and determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number. Further, the examiner concludes that it would be obvious to apply the mathematical relationship taught in Section 5.3 of Menezes to the prime number generated by Section 4.4.1 of Menezes. Use of the one-way function when applied to two prime numbers has the advantageous result of making it more difficult to determine the function inverse, as discussed in the Office Action.

However, this result is significantly different than the extraordinary result of the claimed invention, which produces idem-random numbers in such a manner that it is impossible (not merely difficult) to determine which two original prime or prime-like numbers were used to generate the idem-random number, even if the function which was applied to those original numbers is known. This is because many distinct sets of prime (or prime-like) numbers when operated on by the known function will generate the same output number. Given any finite-length sequence of output values and a known function being applied to sequential numbers, an infinite number of sequences of prime or prime-like numbers could have generated that finite-length output sequence. Therefore, it is impossible to determine which set of prime or prime-like numbers were used as input numbers. As a result, the next output value in the sequence cannot be determined, since it depends on an input number that is not determinable. Menezes does not teach that using a sequence of prime numbers and applying a mathematical relationship will generate a sequence of output numbers for which the next number in the output sequence cannot be accurately predicted. This extraordinary and useful result is achieved by the claimed invention, but not by the processes taught in Menezes.

Furthermore, Menezes does not suggest that there would be any value to using prime or prime-like numbers as input numbers in the course of creating pseudo-random numbers. Instead, Menezes selects a random seed number, and then increments that seed by the value of a single unit (i.e. the number one) to determine the subsequent number to which a function is applied, in contrast to the instant invention which requires each input number to be prime or prime-like. Even if Menezes were to start with a prime number as a seed number, the sequence of subsequent input numbers, being created by sequentially adding single unit-valued numbers, would clearly include many non-prime numbers. (See Menezes Sections 5.3 and 5.2ii). As a result, while Menezes relies on fairly complex mathematical transformations of simple sequences of numbers to generate pseudo-random numbers, idem numbers can be easily and unpredictably created with relatively simple functions applied to sequences of prime or prime-like numbers.

Menezes teaches in Section 5.3 that a function such as SHA-1 or MD5 would be a suitable one-way

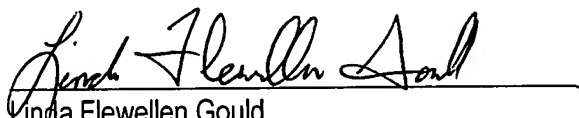
function to create pseudo-random numbers. Subsequent to the publication of Menezes, it has been demonstrated the results of applying the MD5 function can be predicted by a technique implemented on a notebook computer within one minute (See accompanying article Vlastimil Klima: *Tunnels in Hash Functions: MD5 Collisions Within a Minute*, Cryptology ePrint Archive: Report 2006/15, revised 17 April 2006, <http://eprint.iacr.org/2006/105.pdf>). A practical manner of breaking the SHA-1 hash function is also considered feasible (See accompanying article Heise Security News: *SHA-1 Hash Function Under Pressure*, 24 August 2006, <http://www.heise-security.co.uk/news/77244>). Thus, the process described in Menezes is likely to result in predictable pseudo-random numbers, in contrast to the extraordinary results of the claimed invention.

The effectiveness of the Menezes process of generating pseudo-random numbers relies heavily on the ability of the chosen mathematical function to result in unpredictable numbers. However, since one of the functions suggested by Menezes (MD-5) has subsequently been proven to be predictable, it appears that the Menezes process would not reliably result in a useful set of pseudo-random numbers. While Menezes is skilled in the art of creating useful pseudo-random numbers, the process he teaches for achieving that goal does not consistently succeed. In contrast, the claimed invention produces a useful set of unpredictable idem-random numbers, in a manner which was not obvious to Menezes nor taught by him.

The Office Action sites Menezes for the proposition that a random number can be generated by using many sources and then sampling the sources (Menezes Section 5.2). Thus, Menezes obscures the relationships between output pseudo-random numbers and their inputs through sampling to prevent the input numbers from being discovered. In contrast, the claimed invention does not utilize sampling. The relationship between output idem-random numbers and the input numbers used to create them can be fully divulged without allowing a third party to determine the input numbers used in the claimed process and apparatus. Thus, the claimed invention has a clearly advantageous result when compared to the teaching of Menezes.

In view of the above, it is submitted that the claims are in condition for allowance. Allowance of claims 1 - 12 at an early date is solicited.

Respectfully submitted,

A handwritten signature in cursive script, reading "Linda Flewellen Gould", is written over a horizontal line.

Linda Flewellen Gould

Registration Number 31,515

Gould & Whitley

1665 Briargate Blvd., Suite 101

Colorado Springs, CO 80920

Telephone: (719) 531-0994

Fax: (719) 531-0996

Email: lgould@rwsoft.com



Marked Copy
of Claims
10/666,596

1. (Currently Amended) A method of generating an idem-random method comprising the steps of:
 - a. Establishing an initial prime number;
 - b. Establishing a subsequent prime number identification condition;
 - c. Determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number;
 - d. Identifying a mathematical relationship to be applied to said initial prime number and said subsequent prime number;
 - e. Applying said mathematical relationship to said initial prime number and said subsequent prime number to generate an idem-random number for use in an application which can employ random numbers.
2. (Currently Amended) A method of generating a plurality of idem-random numbers, said method comprising the steps of:
 - a. Establishing an initial prime number;
 - b. Establishing a subsequent prime number identification condition;
 - c. Determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number;
 - d. Determining at least one further subsequent prime number satisfying the subsequent prime number identification condition applied to a previously determined subsequent prime number;
 - e. Identifying a mathematical relationship to be applied to a plurality of numbers selected from a set of numbers including said initial prime number and said subsequent prime numbers;
 - f. Applying said mathematical relationship to a first subset of numbers selected from said set of numbers to generate a first idem-random number for use in an application which can employ random numbers;
 - g. Applying said mathematical relationship to a second subset of numbers selected from said set of numbers to generate a subsequent idem-random number for use in an application which can employ random numbers.

3. (Original) A method of generating a plurality of idem-random numbers according to claim 2, wherein said steps d. through g. are repeated to generate a desired number of idem-random numbers.
4. (Original) A method according to claim 2, further comprising the steps of:
 - h. Establishing desired distribution characteristics;
 - i. Determining a distribution operation to be applied to said idem-random numbers to create said desired distribution; and
 - j. Applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers.
5. (Original) A method according to claim 3, further comprising the steps of:
 - h. Establishing desired distribution characteristics;
 - i. Determining a distribution operation to be applied to said idem-random numbers to create said desired distribution; and
 - j. Applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers.
6. (Currently Amended) A method of generating an idem-random number, said method comprising the steps of:
 - a. Specifying particular prime-like characteristics to be satisfied;
 - b. Establishing an initial prime-like number which satisfies said prime-like characteristics;
 - c. Establishing a subsequent prime-like number identification condition;
 - d. Determining a first subsequent prime-like number satisfying the subsequent prime-like number identification condition applied to the initial prime-like number;

- e. Identifying a mathematical relationship to be applied to said initial prime-like number and said subsequent prime-like number;
- f. Applying said mathematical relationship to said initial prime-like number and said subsequent prime-like number to generate an idem-random number for use in an application which can employ random numbers.

7. (Currently Amended) A method of generating a plurality of idem-random numbers, said method comprising the steps of:

- a. Specifying particular prime-like characteristics to be satisfied;
- b. Establishing an initial prime-like number which satisfies said prime-like characteristics;
- c. Establishing a subsequent prime-like number identification condition;
- d. Determining a first subsequent prime-like number satisfying the subsequent prime-like number identification condition applied to the initial prime-like number;
- e. Determining at least one further subsequent prime-like number satisfying the subsequent prime-like number identification condition applied to a previously determined subsequent prime-like number;
- f. Identifying a mathematical relationship to be applied to a plurality of prime-like numbers selected from a set of numbers including said initial prime-like number and said subsequent prime-like numbers;
- g. Applying said mathematical relationship to a first subset of numbers selected from said set of numbers to generate a first idem-random number for use in an application which can employ random numbers;
- h. Applying said mathematical relationship to a second subset of numbers selected from said set of numbers to generate a subsequent idem-random number for use in an application which can employ random numbers.

8. (Original) A method of generating a plurality of idem-random numbers according to claim 7, wherein said steps d. through g. are repeated to generate a desired number of idem-random numbers.

9. (Original) A method according to claim 7, further comprising the steps of:
- h. Establishing desired distribution characteristics;
 - i. Determining a distribution operation to be applied to said idem-random numbers to create said desired distribution; and
 - k. Applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers.
10. (Original) A method according to claim 8, further comprising the steps of:
- h. Establishing desired distribution characteristics;
 - i. Determining a distribution operation to be applied to said idem-random numbers to create said desired distribution; and
 - j. Applying said distribution operation to said idem-random numbers to generate specifically distributed idem-random numbers.
11. (Currently Amended) An apparatus for generating an idem-random number, said apparatus comprising:
- a. Initial prime number establishment means for establishing an initial prime number;
 - b. Subsequent prime number identification condition means for establishing a subsequent prime number identification condition;
 - c. Determination means for determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number;
 - d. Mathematical relationship identification means for identifying a mathematical relationship to be applied to said initial prime number and said first subsequent prime number;

- e. Calculation means for applying said mathematical relationship to said initial prime number and said first subsequent prime number to generate an idem-random number for use in an application which can employ random numbers.

12. (Currently Amended) An apparatus for generating a plurality of idem-random numbers, said apparatus comprising:

- a. Initial prime number establishment means for establishing an initial prime number;
- b. Subsequent prime number identification condition means for establishing a subsequent prime number identification condition;
- c. First determination means for determining a first subsequent prime number satisfying the subsequent prime number identification condition applied to the initial prime number;
- d. Second determination means for determining at least one further subsequent prime number satisfying the subsequent prime number identification condition applied to a previously determined subsequent prime number;
- e. Mathematical relationship identification means for identifying a mathematical relationship to be applied to a plurality of numbers selected from a set of numbers including said initial prime number and said subsequent prime numbers;
- f. First calculation means for applying said mathematical relationship to a first subset of numbers selected from said set of numbers to generate a first idem-random number for use in an application which can employ random numbers;
- g. Second calculation means for applying said mathematical relationship to a second subset of numbers selected from said set of numbers to generate a subsequent idem-random number for use in an application which can employ random numbers.